Claims

1. A security server system that securely qualifies the execution of programs within a community of networked host computer systems, said security server system comprising:

a) a database storing sets of pre-qualified program signatures and defined policy rules associating execution permission qualifiers with execution control values; and

b) a processor coupled to said database and including a memory storing a control program and a communications network interface coupleable to a community of one or more host computer systems, said processor operative to execute said control program in response to execution requests received via said communications network interface from identifiable host computer systems within said community, wherein a predetermined execution request received from a predetermined host computer system includes an identification of a program load request, request context related data, and a secure program signature, execution of said control program providing for determination of an execution control value based on an evaluation of said predetermined execution request relative to said sets of pre-qualified program signatures and defined policy rules, whereby return of said execution control value to said predetermined host computer system securely qualifies the execution of the program identified with said program load request.

2. The security server system of Claim 1 wherein each identifiable host computer within said community includes an local operating system, said security

server system further comprising a module implemented on each identifiable host computer system within said community in combination with said local operating systems, said module, responsive to said program load request, being operative to generate said predetermined execution request, said module, responsive to an execution request response including said execution control value, being operative to permit or deny said program load request.

3. The security server system of Claim 2 wherein execution of said control program provides for the lookup of said secure program signature in said database to identify a resource reference that is evaluated with said predetermined execution request to determine said execution control value.

4. The security server system of Claim 3 wherein said predetermined execution request includes authentication data and access attributes determined from said local operating system relative to said program load request.

5. The security server system of Claim 4 wherein execution of said control program provides for the selection of a default resource reference on a failure of the lookup of said secure program signature in said database, said default resource reference being evaluated with said predetermined execution request to determine said execution control value.

6. The security server system of Claim 5 wherein said execution control value provides a specification to permit or deny said program load request and wherein

said specification to permit is selectively qualifiable to include predetermined execution limitations including first limitations on said program load request.

7. The security server system of Claim 6 wherein said predetermined execution limitations include second limitations on the execution of the program identified with said program load request.

8. The security server system of Claim 7 wherein said module, responsive to said execution control value, is operative to implement said predetermined execution limitations.

9. A security server system that securely controls load execution of programs on a host computer system, said security server system comprising:

a) a module installed as a component of a host computer system, said module operative relative to an operating system executed by said host computer system to intercept system calls to load an execute program for execution, said module further operative to generate a security request containing a predetermined load request, associated authentication data and access attributes and a target secure program signature of an executable program identified by said predetermined load request; and

b) a security server, responsive to said security request, including a first database of pre-qualified secure program signatures and a second database of policy rules associating defined load requests, authentication data, and access attributes with predetermined pre-qualified secure program signatures, said security server further including a control program operative to parse said policy

rules relative to said security request and generate a security request response reflective of a match between said security request and a corresponding one of said policy rules.

10. The security server system of Claim 9 wherein said module is responsive to said security request response to enable completion of said predetermined load request by said operating system.

11. The security server system of Claim 10 wherein said control program is operative to lookup said target secure program signature in said first database to obtain a resource reference, wherein said control program is operative to lookup said predetermined load request, associated authentication data and access attributes, and said resource reference in said second database to identify an applicable set of policy rules, and wherein said control program is operative to generate said security request response based on said applicable set of policy rules.

12. The security server system of Claim 11 wherein said applicable set of policy rules includes a default policy rule corresponding to a lookup failure of said target secure program signature in said first database.

13. The security server system of Claim 9 wherein said module and security server are interconnected by a communications network through which said security request is transmitted.

14. A method of securing the execution of programs on a host computer system comprising the steps of:

a) intercepting, on a host computer, a load request for the execution of a program;

b) determining authorization data and access attributes associated with said load request;

c) generating a secure signature for said program;

d) providing a security request, including an identification of said load request, said authorization data and access attributes and said secure signature, to a security server, wherein said security server, in secure isolation from said host computer system, evaluates said security request and returns a security request response; and

e) selectively enabling performance of said load request dependent on said security request response.

15. The method of Claim 14 wherein said security server performs the steps of:

a) evaluating said security request to determine whether said secure signature matches any of a plurality of predetermined secure signatures maintained in a first database by said security server and whether said identification of said load request and said authorization data and access attributes match any of a plurality of policy rules maintained in a second database by said security server; and

b) generating said security request response dependent on said step of evaluating.

16. The method of Claim 15 wherein said security server further performs the step of parsing a policy rule identified by said step of evaluating to implement the policy operation identified by said policy rule, wherein said step of generating said security request response is further dependent on said step of parsing.

17. The method of Claim 16 wherein said step of generating identifies in said security request response a control directive having at least the possible values of deny, enable, and enable subject to limitations.

18. The method of Claim 17 wherein said step of selectively enabling performance includes the step of constraining execution of said program dependent on said control directive.